



Europäisches Patentamt
European Patent Office
Office européen des brevets

⑯ Veröffentlichungsnummer:

0 098 437
A2

⑯

EUROPÄISCHE PATENTANMELDUNG

㉑ Anmeldenummer: 83105968.8

㉓ Int. Cl.³: E 05 B 49/00, G 07 F 7/08

㉒ Anmeldetag: 18.06.83

㉔ Priorität: 09.07.82 DE 3225754

㉕ Anmelder: Hülsbeck & Fürst GmbH. & Co. KG, Steeger
Strasse 17, D-5620 Velbert 1 (DE)

㉖ Veröffentlichungstag der Anmeldung: 18.01.84
Patentblatt 84/3

㉗ Erfinder: Stellberger, Karl-Heinz,
Jacob-Lüneschloss-Strasse 8, D-5620 Velbert 15 (DE)

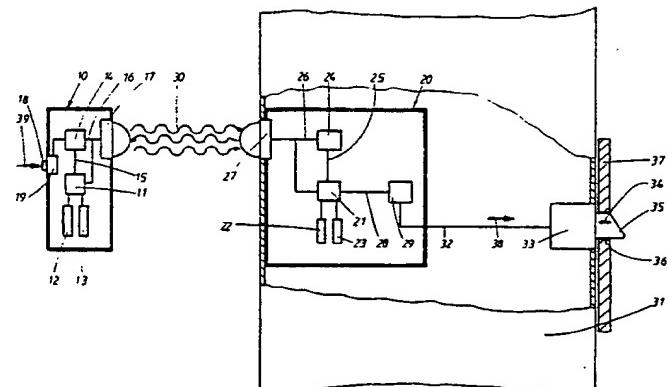
㉘ Benannte Vertragsstaaten: DE FR GB IT NL SE

㉙ Vertreter: Mentzel, Norbert, Dipl.-Phys. et al,
Patentanwälte Dipl.-Phys. Buse Dipl.-Phys. Mentzel
Dipl.-Ing. Ludewig Unterdörnen 114,
D-5600 Wuppertal 2 (DE)

㉚ Elektronische Schließseinrichtung mit über elektrische Impulse miteinander in Wechselwirkung tretenden, schlüsselartigen und schlossartigen Teilen.

㉛ Bei einer Schließeinrichtung mit elektrisch miteinander in Wechselwirkung tretenden Schlüsselteilen (10) und Schloßteilen (20), die durch eine innere, elektronische Kodierung gegenüber anderen Schlüssel- und Schloßteilen individualisiert sind, soll eine hohe Variationsvielfalt und ein schwerer Nachbau des Schlüsselteils durch Unbefugte erreicht werden und im Falle eines Spannungsabfalls an der schloß- bzw. schlüsselseitigen Energiequelle soll eine Abstimmung im Arbeitsrhythmus des Schloß- und Schlüsselteils entbehrlich sein. Dazu wird vorgeschlagen, als Eingangsgrößen für eine elektronische Kodierung lediglich eine Teilmenge willkürlich generierter Zufallszahlen zu verwenden und die elektronische Kodierung für zusammengehörige Schlüssel- und Schloßteile (10, 20) zweistufig auszubilden. In einer ersten Stufe wird eine Rechenoperation nach einem bestimmten Algorithmus durchgeführt. In einer zweiten Stufe wird lediglich ein Bruchstück des Rechenresultats nach einer bestimmten Regel entnommen und als Ausgangsgröße einem Vergleicher zugeführt, wo die schloß- und schlüsselseitig anfallenden Bruchstücke auf ihre Übereinstimmung überprüft werden.

Liegt Übereinstimmung vor, so wird ein Schaltimpuls abgegeben, der die Sperrmittel im Schloßteil umsteuert.



EP 0 098 437 A2

PATENTANWÄLTE 0098437
DIPL.-PHYS. BUSE · DIPL.-PHYS. MENTZEL · DIPL.-ING. LUDEWIG
Unterdörnen 114 · Postfach 200210 · 5600 Wuppertal 2 · Fernruf (0202) 557022/23/24 · Telex 8591606 wpat

57

5600 Wuppertal 2, den

Kennwort: "MP-Schließeinrichtung"

Firma Hülsbeck & Fürst GmbH & Co. KG,
Steeger Str. 17, D-5620 Velbert 1
(Bundesrepublik Deutschland)

Elektronische Schließeinrichtung mit über elektrische Impulse miteinander in Wechselwirkung tretenden, schlüsselartigen und schloßartigen Teilen

Die Erfindung bezieht sich auf eine Schließeinrichtung der im Gattungsbegriff des Anspruches 1 (Seite 24, Zeile 1 bis Seite 25, Zeile 14) angegebenen Art.

Bei der bekannten Schließeinrichtung dieser Art

5 (DE-A 22 34 815; US-A 37 61 892) befindet sich der Startschalter am Schloßteil, nach dessen Betätigung ein Oszillator mit einem Zählwerk alle möglichen Permutationen eines Zahlensystems durchspielt und den gesamten "Zahlenkörper" in Form elektrischer Impulse an ein ROM sowohl im Schloßteil als auch im damit kontaktierten Schlüsselteil weitergibt. Diese Impulsfolge bestimmt die Eingangsgrößen für die beiden ROMs.
10 Unter diesen Adressen hat jeder ROM in eindeutiger Weise eine Ausgangsgröße gespeichert, die er an einen von zwei Eingängen eines Vergleichers wieder in Form elektrischer Impulse abgibt. Vom Vergleicher werden die schlüssel- und schloßseitig anfallenden Ausgangsgrößen auf Übereinstimmung geprüft und ein daran angeschlossenes elektromechanisches Gerät nur dann umgesteuert, wenn die beiden geprüften Ausgangsgrößen übereinstimmen. Der besondere Speicherinhalt
15 der beiden ROMs ist die Kodierung des zusammenge-
20

hörigen Schlüssel- und Schloßteils in elektronischer Form, durch welche dieser Schlüssel- und Schloßteil gegenüber allen übrigen individualisiert ist und sich denen gegenüber unterscheidet. Die Ausgangsgrößen dieser
5 ROMs ist wiederum eine eindeutige Zahl dieses "Zahlenkörpers".

Nachteilig ist bei dieser bekannten Schließeinrichtung die verhältnismäßig leichte Kopierbarkeit des Schlüssel-
10 teils. Eine unbefugte Person kann durch Betätigen des Startschalters am Schloßteil die ganze Impulsfolge aufnehmen und, wenn sie kurzzeitig in den Besitz des zugehörigen Schlüsselteils kommt, ebenfalls aufzeichnen, welche Folge von Ausgangsgrößen der Schlüsselteil darauf
15 abgibt. Der elektronische Kode ist damit "geknackt": Die unbefugte Person kann danach einen Nachschlüssel leicht herstellen. Durch Verwendung eines sehr großen "Zahlenkörpers" für die Eingangs- und Ausgangsgrößen lässt sich die Aufbruchsicherheit dieser bekannten
20 Schließeinrichtung nicht nennenswert erhöhen und man bekommt dabei den Nachteil eines großen Zeitaufwands für die Übermittlung langer Impulsfolgen.

Bei Übertragungsvorgängen von Daten zwischen zwei
25 Stationen (EP-A 0 002 580) ist es zwar bekannt, in der ersten Station eine Zufallszahl zu generieren, doch wird eine davon abgeleitete verschlüsselte Prüfzahl zur zweiten Station übertragen, wo eine Entschlüsselung vorgenommen wird. Die Kommunikation zwischen den beiden
30 Stationen findet durch ein umständliches Chiffrieren und Dechiffrieren statt. Die Anwendung dieser Datenübertragung auf Schließeinrichtungen mit individuell kodierten Schlüssel- und Schloßteilen ist ungünstig.

Gleiches gilt für eine andere Anlage zur Nachrichtenübertragung (DE-A 22 53 275), deren Zugang durch Unbefugte dadurch gesichert werden soll, daß außer einem elektronischen Schlüssel noch ein Kodewort eingegeben wird.

- 5 In der Anlage werden zwar eine Gruppe von Zufallszahlen erzeugt, doch dienen diese nur dazu, auf beiden Seiten einen bestimmten Kode auszuwählen. Letzteres wird auch für Schließeinrichtungen von Schloß- und Schlüsselteilen verwendet (DE-B 26 35 180; US-A 42 09 782), wo
- 10 nach einem Zufallsgesetz die elektronische Kodierung in einem Schlüssel-Schloß-Paar verändert wird. Ist bei Anwendung die Übereinstimmung des Kodes festgestellt worden, so wird dem Schlüssel- und Schloßteil ein neues Kode-Paar eingegeben. Hier bildet die Zufallszahl unmittelbar den elektronischen Kode, der sich nach jeder Benutzung im Schlüssel- und Schloßteil verändert.

- Der Erfindung liegt die Aufgabe zugrunde, eine elektronische Schließeinrichtung mit hoher Aufbruchsicherheit
- 20 der im Gattungsbegriff des Anspruches 1 angegebenen Art zu entwickeln, bei welcher der Schlüsselteil schwer zu kopieren ist und der Schlüssel- und Schloßteil auch dann, wenn die schlüssel- bzw. schloßseitige Energiequelle zeitweise ausfallen sollte, ohne erneute Abstimmung ihrer Arbeitsrhythmen weiter funktionsfähig bleiben.

- Dies wird erfindungsgemäß durch die im Kennzeichen des Anspruches 1 (Seite 25, Zeile 16 bis Seite 26, Zeile 10) angeführten Maßnahmen erreicht. Durch die zweistufig ausgebildete elektronische Kodierung wird einerseits eine sehr große Variationsvielfalt zur Herstellung sehr unterschiedlicher Schlüssel- und Schloßteile erreicht und andererseits eine hohe Aufbruchsicherheit erzielt, obwohl nur eine beschränkte Menge von Eingangsgrößen verwendet
- 30 wird, die sich schnell übertragen lassen. Die Eingangsgrößen sind nämlich

Zufallszahlen, die ganz willkürlich aus einem großen "Zahlenkörper" entnommen werden. Bei jeder Benutzung ergeben sich ganz andere Zufallszahlen, so daß auch nach sehr langer, mühevoller Beobachtung nicht alle 5 möglichen Eingangsgrößen durchgespielt worden sind. Es nützt auch einer unberechtigten Person nichts, wenn sie die Ausgangsgrößen auf bestimmte Eingangsgrößen aufgezeichnet hat, denn es ist nicht voraussehbar, welche Zufallszahlen in welcher Reihenfolge im Schloß- 10 teil generiert werden, wenn ein Start vom Schlüsselteil ausgeht. Es wird daher mit Sicherheit eine imitierte Folge von Ausgangsgrößen falsch sein, wenn man sie einem Schloßteil zuspielt. Die Signalübergänge zwischen dem Schlüssel- und Schloßteil lassen auch 15 keine Rückschlüsse auf die feststehende elektronische Kodierung der erfindungsgemäßen Schließeinrichtung zu, was auch für die Ausgangsgrößen gilt. Dies liegt in der besonderen Zweistufigkeit der erfindungsgemäßen Kodierung. Der Algorithmus der ersten Stufe ist sehr 20 einfach und errechnet für die jeweils anfallende Zufallszahl, die aus einem sehr umfangreichen "Zahlenkörper" willkürlich entnommen wird, mittels einer Funktionsgleichung ein eindeutiges Rechen-Resultat. Dieses wird aber nicht übermittelt, sondern lediglich ein Bruchstück davon, 25 welches in einer zweiten Stufe der Kodierung nach einer bestimmten Regel aus dem vorhergehenden Rechen-Resultat ermittelt wird. Diese Regel kann z.B. darin bestehen, daß nur ganz bestimmte Stellen der Zahl im Rechen-Resultat als zu übermittelnde Ausgangsgrößen verwendet werden, z.B. die 30 zweite, fünfte und siebte Stelle der ermittelten Zahl, wobei die Reihenfolge dieser Stellen in sich noch nach einer bestimmten Regel vertauscht sein kann. Eine Dechiffrierung der Ausgangsgrößen erfolgt dabei nicht, denn der zum

Schlüsselteil zugehörige Schloßteil arbeitet mit dem gleichen zweistufigen Kode. Am Vergleicher werden lediglich die, keine Rückschlüsse zulassenden, verschleierten Ausgangsgrößen des Schloß- und Schlüsselteils miteinander verglichen. Fällt die elektrische Energiequelle im Schlüssel- oder Schloßteil aus, so ist die zweistufige Kodierung davon nicht betroffen; ein Zurückstellen der Programme im Schlüssel- und Schloßteil ist nicht erforderlich. Ist die elektrische Energieversorgung wieder hergestellt, so kann bei erneutem, vom Schlüsselteil ausgehenden Start eine gegenseitige, vom Vergleicher bewirkte "Abtastung" zwischen dem jeweils benutzten Schlüssel- und Schloßteil dahingehend erfolgen, ob die nach außen völlig unbekannt bleibende, innere zweistufige Kodierung übereinstimmt oder nicht. Durch Änderung des Algorithmus und der Regel zur Bestimmung des Bruchstücks vom Rechen-Resultat lässt sich eine sehr große Vielzahl von gut unterscheidbaren Schlüssel-Schloß-Paaren entwickeln. Die Variationsvielfalt der erfindungsgemäßen Schließeinrichtung ist daher sehr groß.

Im Rahmen der Erfindung ist es möglich, den Vergleich der anfallenden Ausgangsgrößen in mehreren aufeinanderfolgenden Arbeitszyklen auszuführen, von denen jeder 25 eine solche zweistufige Ermittlung von Ausgangsgrößen beinhaltet. Dabei werden für jeden Arbeitszyklus eine Gruppe von Zufallszahlen verwendet, die zweckmäßigerweise aus einem gegebenen Vorrat von Zufallszahlen entnommen wird und die jeweils nach einem bestimmten Bildungsgesetz schlüssel- und schloßseitig zu einer Rechengröße zusammengesetzt werden. Dieses Bildungsgesetz bietet ein weiteres Element zur Kodierung eines zusammengehörigen Schlüssel-Schloß-Paars. Bei solchen mehrfachen Arbeitszyklen für die Wechselwirkung zwischen dem Schlüssel- und Schloß-

teil werden zweckmäßigerweise in einem Vorprogramm gleich eine größere Menge von Zufallszahlen zwischen dem Schlüssel- und Schloßteil übermittelt und jeweils gespeichert, um für die nachfolgende Ermittlungsarbeit der jeweiligen Ausgangsgrößen in jedem Arbeitszyklus zur Verfügung zu stehen. Um die Entschlüsselung zu erschweren ist es dabei sehr vorteilhaft, diese Gruppe von Zufallszahlen sowohl im Schlüssel- als auch im Schloßteil von einander unabhängig zu generieren und dann einander mit-
5 zuteilen. Die Arbeit wird in den aufeinanderfolgenden Arbeitszyklen nur dann fortgesetzt, wenn in jedem Zyklus eine Übereinstimmung der schloß- und schlüsselseitig angefallenen Ausgangsgrößen ermittelt wird. Der bei Übereinstimmung anfallende Schaltimpuls wirkt, solange nicht
10 der letzte Arbeitszyklus erreicht ist, noch nicht unmittelbar mit den schloßartigen Sperrmitteln, sondern löst die Bildung einer neuen Rechengröße aus einer bestimmten Gruppe der gespeicherten Zufallszahlen aus, die
15 für die Ermittlung der Ausgangsgröße im nächsten Arbeits-
20 zyklus verwendet wird.

Durch die Aufeinanderfolge mehrerer Arbeitszyklen wird eine außerordentlich hohe Sicherheit zur Unterscheidung verschiedener Schlüssel-Schloß-Paare erreicht. Die
25 Vergleichsphase zwischen den in jedem Arbeitszyklus angefallenen Ausgangsgrößen wird zweckmäßigerweise abwechselnd einmal im Schlüssel- und dann im Schloßteil ausgeführt, weshalb die Wechselwirkung zwischen dem Schlüssel- und Schloßteil in aufeinanderfolgenden
30 Arbeitszyklen jeweils spiegelbildlich zueinander abläuft; einmal ist der Schlüsselteil und einmal der Schloßteil der aktive Teil, der die angefallenen Ausgangsgrößen auf ihre Übereinstimmung prüft. Dadurch ist ein besonders hohes Maß an Aufbruchsicherheit gegeben.

Die Aufbruchsicherheit läßt sich weiterhin dadurch erhöhen, daß man in aufeinanderfolgenden Arbeitszyklen auch noch den Algorithmus, die Regel zur Bildung des Rechen-Resultats-Bruchstücks und/oder das Bildungs-
5 gesetz für die Rechengröße zyklenweise verändert. Dies erschwert die Dekodierung der erfindungsgemäßen Schließeinrichtung durch Unbefugte.

Zur weiteren Erhöhung der Aufbruchsicherheit wird zweckmäßigerweise der Schlüssel- und/oder Schloßteil für
10 wenigstens eine bestimmte Zeitdauer unwirksam gesetzt, falls in einem vorausgehenden Arbeitszyklus keine Übereinstimmung der schloß- und schlüsselseitig angefallenen Ausgangsgrößen festgestellt wird. Der nächste Arbeits-
15 zyklus beginnt dann nicht mehr. Die Schließeinrichtung wird erst nach Ablauf dieser Zeitdauer wieder wirksam. Damit wird verhindert, daß zu Aufbruchzwecken eine Vielzahl von Probesignalen abgegeben werden kann, um die erfindungsgemäße Schließeinrichtung zu "knacken". Sobald
20 ein Fehler auftritt, ist die Schließeinrichtung unwirksam gesetzt und arbeitet nicht mehr weiter.

Zur Kommunikation zwischen dem Schlüssel- und Schloßteil können zwar die elektrischen Impulse durch Berührungs-
25 kontakt übermittelt werden, doch empfiehlt es sich, diese durch Strahlung zu übertragen, weil dies bereits aus einer größeren Entfernung geschehen kann und mechanische Beschädigungen ausschließt.

30 Das erfindungsgemäße Schließsystem eignet sich auch bequem dazu, bei Anlagen mit hierarchisch einander über- und untergeordneten Schlüssel- und Schloßteilen anzuwenden, wie bei Haupt- und Nebenschlüsseln. Es kann dabei

so verfahren werden, daß allen Schlüssel- und Schloß-
teilen der gleiche Algorithmus zugrunde gelegt wird,
aber ein untergeordneter Schlüssel- und Schloßteil sich
gegenüber dem übergeordneten dadurch unterscheidet, daß
5 nur ein kürzeres Bruchstück der Ausgangsgröße für den
Vergleich übermittelt wird. Der Generalhauptschlüssel
und sein Schloßteil liefern demnach das volle Bruchstück
des Rechenresultats als Ausgangsgröße. Je untergeordneter
der Schlüssel- und Schloßteil ist, um so kürzere Bruch-
10 stücke werden als Ausgangsgrößen übermittelt und mit-
einander verglichen. Weitere Maßnahmen und Vorteile der
Erfindung ergeben sich aus den Unteransprüchen, den
Zeichnungen und der nachfolgenden Beschreibung.

In den Zeichnungen und Tabellen ist die Erfindung in zwei Ausführungsbeispielen dargestellt. Es zeigen:

Fig. 1 in schematischer Darstellung und aufgebrochen gezeichnet, die zum erfindungsgemäßen Schließsystem gehörenden beiden schlüsselartigen und schloßartigen Teile,
5

Tabelle I das Vergleichsprogramm einer ersten Schließeinrichtung und
10

Tabelle II das Vergleichsprogramm einer weiteren, abgewandelt ausgebildeten Schließeinrichtung.

15 Die Schließeinrichtung besteht aus einem schlüsselartigen Teil 10 und einem schloßartigen Teil 20, die nachfolgend abgekürzt Schlüssel und Schloß benannt werden sollen. Beide Teile 10, 20 beinhalten elektronische Mikroprozessoren, die man gliedern kann, in einen Mikroprozessor 11, 21 an
20 die ein fester Speicher 12, 22 und ein zur Aufnahme von Zwischenergebnissen dienender flüchtiger Speicher 13, 23 angeschlossen sind. Die Stromversorgung dieser Bauteile ist nicht näher gezeigt und kann über eine elektrische Batterie od.dgl. erfolgen. Als Besonderheit beinhalten Schlüssel
25 10 und Schloß 20 je einen Zufallszahlengenerator 14, 24, der über die Leitung 15 bzw. 25 einerseits mit dem zugehörigen Mikroprozessor 11, 21 und über die Leitung 16, 26 je an ein Kommunikationsglied 17, 27 andererseits angeschlossen ist. Die Kommunikationsglieder 17, 27 könnten zwar durch Kontaktberührung miteinander in Wechselwirkung treten, doch sind sie im dargestellten Ausführungsbeispiel bereits in einer Abstandslage zueinander wirksam, weil sie als Strahlungsempfänger und Strahlungssender ausgebildet sind, z.B. zur Übertragung von elektromagnetischer Strahlung, insbesondere Infrarotstrahlung. Denkbar wäre es, auch
30
35

andere Strahlungsarten, z.B. Ultraschall, zur Signalübertragung zu verwenden. Durch die Kommunikationsglieder 17, 27 sind Schlüssel 10 und Schloß 20 in der Lage, in Form einer Frage und einer Antwort Informationen auszutauschen,
5 mit denen das Schloß 20 feststellen kann, daß der ihm zugeordnete, ordnungsgemäße Schlüssel 10 vorliegt. Aus Sicherheitsgründen kann auch eine Überprüfung seitens des Schlüssels erfolgen, ob das ordnungsgemäße Schloß 20 ihm vorliegt. Diese Überprüfungen können mehrfach
10 erfolgen, wodurch eine hohe Sicherheit erzielt wird. Die verschiedenen Signalübergänge 30 im Kontaktmedium zwischen den Kommunikationsgliedern 17, 27 sind in Fig. 1 und in den nachfolgend noch näher zu beschreibenden Tabellen I, II durch Wellen 30 angedeutet.

15 Das Schloß 20 ist fest in einem abzuschließenden Element, z.B. einer Fahrzeugtür 31, eingebaut. Der Schlüssel 10 hat ein bequemes Hosentaschenformat und kann von einer Bedienungsperson mitgenommen werden. Zur Auslösung einer
20 Wechselwirkung zwischen Schlüssel und Schloß ist der Schlüssel 10 mit einem von einer Handhabe 18 betätigbaren Auslöseglied 19 versehen, welches mit dem Zufallszahlengenerator 14 bzw. dem Mikroprozessor 11 verbunden ist. Liegt die noch näher zu beschreibende Übereinstimmung zwischen
25 Schlüssel und Schloß 10, 20 vor, so gibt der schloßseitige Mikroprozessor 21 über die Leitung 28 ein Signal an ein Schaltglied 29, welches über eine Verbindungsleitung 32 mit einem Stellwerk 33 in Wirkverbindung steht, das auf einen im Sinne des eingeziehenen Pfeiles
30 34 ein- und ausverschieblichen Riegel 35 einwirkt. In der gezeigten Ausschublage von Fig. 1 greift der Riegel 35 sperrwirksam in die Öffnung 36 eines am feststehenden Rahmen der Tür befindlichen Schließblechs 37 ein. Die Tür 31 befindet sich in der Sperrlage.

Durch Einwirken des ordnungsgemäßen Schlüssels 10 gibt das Schaltglied 29 einen Schaltimpuls gemäß dem angedeuteten Pfeil 38 von Fig. 1 über die Verbindungsleitung 32 an das Stellwerk 33 ab, welches umgesteuert wird und den Riegel 5 35 in seine Einschublage bringt, wo er aus der Öffnung 36 zurückgezogen ist und das Schließblech 37 freigibt. Es liegt die Offenstellung des Schlosses 20 vor; die Tür 31 kann aufgeschwenkt werden.

- 10 Nach seiner Umsteuerung durch den Schaltimpuls 38 könnte der Riegel 35 selbsttätig durch eine Rückstellfeder od.dgl. wieder in seine Sperrlage von Fig. 1 überführt werden. Es läßt sich natürlich auch ein Stellwerk 33 verwenden, wo für die Umsteuerung des Riegels 35 aus der vorerwähnten 15 Freigabelage in die Sperrlage wieder ein Schaltimpuls 38 erforderlich ist, der durch erneute Wechselwirkung zwischen Schlüssel und Schloß 10, 20 abgegeben wird. Es versteht sich, daß hierzu jedes bekannte Stellwerk 33 mit beliebigem Verschlußorgan anstelle des Riegels 35 verwendet werden 20 könnte, z.B. ein Gabelfallenschloß von Kraftfahrzeugen.

Das Prinzip der Erfindung ist anhand der Tabelle I leicht zu erläutern. Ausweislich der Überschrift sind hier, von oben nach unten gesehen, in zeitlicher Reihenfolge, 25 die Vorgänge eingezeichnet, die, von links nach rechts gesehen, im Schlüssel 10, im Kontaktmedium 30 und im Schloß 20 ablaufen. In der rechten Spalte sind die Bezeichnungen für die einzelnen Arbeitsphasen der in den vorausgehenden Spalten symbolisch angedeuteten Arbeitsvorgänge enthalten 30 und ihre Programmierung angedeutet, deren Unterscheidung für die nachfolgend noch näher zu beschreibende Tabelle II vorteilhaft ist. Damit der Vergleich zwischen den beiden Tabellen I, II leichter fällt, sind beim Ausführungsbeispiel der Tabelle I die Arbeitsphasen nicht 35 mit einer fortlaufenden Buchstabenfolge gekennzeichnet.

In Tabelle II treten nämlich noch zwei zusätzliche Vorgänge ein, für welche diese fehlenden Buchstaben reserviert sind. Dies ist für die Systematik der Beschreibung zweckdienlicher.

5

Nachfolgend wird anhand der Bezeichnungen angegeben, welche Vorgänge in den einzelnen Arbeitsphasen der nach Tabelle I wirksamen Schließeinrichtung gemäß Fig. 1 ablaufen:

10 A.) Auslösung:

Durch Drücken des Startknopfes 18 von Fig. 1 im Sinne des angedeuteten Betätigungspeiles 39 beginnt das im Speicher 12 des Mikroprozessors 11 enthaltene Steuerprogramm selbsttätig abzulaufen.

15

B.) Start-Kommunikation:

Vom Kommunikationsglied 17 des Schlüssels 10 geht ein Startimpuls aus, wird vom schloßseitigen Kommunikationsglied 27 empfangen und aktiviert den dortigen Mikroprozessor 21, 20 der das in seinem Speicher 22 befindliche Programm seinerseits in Gang setzt.

C.) Generieren:

Der im Schloß befindliche Zufallszahlengenerator 24 erzeugt eine beliebige, aber im Einzelfall bestimmte Zufallszahl als Eingangsgröße, z.B. $x = 438$. Ähnliches könnte auch auf Seiten des Schlüssels 10 geschehen, doch soll dies zunächst unberücksichtigt bleiben und insbesondere erst im Zusammenhang mit Tabelle II als weitere Möglichkeit näher beschrieben werden.

D.) Fragen:

Das Kommunikationsglied 27 wirkt jetzt als Sender und übermittelt die Eingangsgröße x an das schlüsselseitige, nunmehr als Empfänger dienende Kommunikationsglied 17

35

durch Infrarotstrahlung 30 als Frage. Damit ist das Programm beendet. Jetzt beginnt das eigentliche Hauptprogramm, das eine zweistufige Kodierung umfaßt.

5 G.) Rechen-Phase:

Unabhängig voneinander wird, also schloß- und schlüsselseitig jeweils für sich, ausgehend von der willkürlichen Eingangsgröße x , anhand einer beidseitig übereinstimmenden Funktionsgleichung $y = f(x)$, die den Algorithmus für die 10 Rechenoperation in dieser ersten Stufe darstellt, eine zugehörige abhängige Veränderliche y errechnet. Diese Funktionsgleichung ist einer erster Kode, der in dieser ersten Stufe zur Individualisierung zusammengehöriger Schlüssel- und Schloßteile gegenüber anderen Schlüssel- 15 und Schloßteilen dient. Handelt es sich beispielsweise im vorliegenden Fall um die Funktionsgleichung $y = \sqrt[4]{x} + 1,507$, so erhält man, bei $x = 438$, als Rechenresultat $y = 6,08176$.

20 H.) Verschleierungs-Phase:

Nach einer schlüssel- und schloßseitig übereinstimmenden Regel wird in der nächsten Stufe ein Bruchstück \bar{y} des ermittelten Rechenresultats y entnommen, das nunmehr als Ausgangsgröße für die weiteren Vorgänge dient. Diese Regel 25 ist so gewählt, daß das vorausgehende Rechenresultat y daraus nicht ableitbar ist und auch keine Rückschlüsse auf die Rechenoperation der vorausgehenden Stufe gemacht werden können. Im vorliegenden Fall soll als Regel gelten, die zweite, dritte, vierte und fünfte Stelle hinter dem Komma 30 der Funktionsgröße y als Ausgangsgröße \bar{y} zu verwenden. Dies ergibt im vorliegenden Fall $\bar{y} = 8176$.

J.) Antworten:

Während die schloßseitig ermittelte Ausgangsgröße \bar{y} im 35 Speicher 23 kurzzeitig festgehalten wird, wird die schlüsselseitig ermittelte Ausgangsgröße \bar{y} als Antwort über die beiden Kommunikationsglieder 17 und 27 wieder dem Schloß 20 übermittelt.

K.) Vergleichen:

Im Schloß 20 werden die schlüssel- und schloßseitig erlangten Ausgangsgrößen \bar{y} auf ihre Identität überprüft. Man kann sich hierzu ein Vergleichsglied verwenden, das, in Abhängigkeit davon, ob Übereinstimmung oder Nichtübereinstimmung vorliegt, zwei Ergebnisse liefert, nämlich:

L.) Auswahl-Folge:

Bei Nichtidentität, die in Tabelle I durch die strichpunktierte Stellung eines symbolischen Schaltglieds ange deutet ist, wird das weitere Vergleichsprogramm auf der Schloßseite abgebrochen, und zwar zweckmäßigerweise für eine bestimmte Zeitdauer, z.B. für 30 Sekunden. Erst dann setzt sich der Mikroprozessor 21 in seine Ausgangslage zurück.

Während dieser Zeitdauer ist das Schloß 20 auf keinerlei schlüsselseitige Impulse ansprechbar. Bedarfsweise könnte das Ausschalten der schloßseitigen Elektronik endgültig sein, so daß weitere Manipulationen am Schloß aufgrund der offensichtlich eingeleiteten Aufbruchsversuche nicht mehr möglich sind; erst besondere fachmännische Maßnahmen bringen das Schloß 20 in seinen anfänglichen Zustand wieder zurück, der ihn für schlüsselseitige Impulse überhaupt erst wieder empfänglich macht.

Im Übereinstimmungsfall dagegen, wenn also die beidseitigen Endgrößen \bar{y} identisch sind, wird vom Schaltglied 29 ein Schaltimpuls 38 ausgelöst, der bei einfachen Schließeinrichtungen bereits unmittelbar zur Umsteuerung des schloßseitigen Riegels 35 dienen kann. Damit ist die Programmfolge der Tabelle I abgeschlossen.

Um eine höhere Aufbruchsicherheit zu erreichen, kann der angefallene Schaltimpuls als Auslöser einer neuen Arbeitsfolge zwischen Schlüssel und Schloß dienen, die in spiegelbildlicher Weise zu der in Tabelle I erwähnten abläuft, was dort nicht näher gezeigt ist.

Über die Kommunikationsglieder 17, 27 kann ein Rückerregen des Schlüssels 10 erfolgen, wo eine weitere Zufallszahl generiert wird, welche in den nachfolgenden Arbeitsphasen die analogen, zu C.) bis L.) entsprechenden Vorgänge
5 vollzieht, die allerdings jetzt in spiegelbildlicher Weise zwischen Schlüssel und Schloß ablaufen. Jetzt würde der Schlüssel 10 der aktive Partner sein, während das Schloß auf dessen Veranlassung passiv mitwirkt. So würde entsprechend C.) der Schlüssel die neu generierten Zufalls-
10 zahlen als Rückfrage an das Schloß weiterleiten, so daß beidseitig, gemäß G.) und H.) die Rechenoperationen ausgeführt werden und gemäß J.) eine Rückantwort des Schlosses an den Schlüssel gelangt, wo diesmal der Vergleich der beidseitigen Ausgangsgrößen stattfindet. Dann er-
15 gibt sich schlüsselseitig entweder ein Stopp der Verfahrensweise wegen Nichtübereinstimmung oder ein schlüsselseitiger Schaltimpuls, der nun seinerseits einen weiteren Arbeitszyklus einleitet, der nun wieder gemäß Tabelle I abläuft. Nach einer Anzahl von Arbeitszyklen ergibt sich schließlich, wenn erfolgreich alle Übereinstimmungen festgestellt
20 wurden, im Schloß 20 ein endgültiger Schaltimpuls, der die Umsteuerung der Sperrmittel 33, 34 des Schlosses 20 bewirkt.

In Tabelle II ist ein in dieser Weise mehrere Arbeitszyklen umfassendes Programm dargestellt, das sich durch eine besonders hohe Variationsvielfalt in der Gestaltung von Schlüssel und Schloß und hohe Aufbruchsicherheit des Schlosses auszeichnet. Zur Bezeichnung entsprechender Arbeitsphasen sind die gleichen Bezeichnungen wie in
25 Tabelle I verwendet worden, aber zur Herausstellung ihrer Besonderheit mit einem Index versehen. Aus der Tabelle II ergibt sich nunmehr, ergänzend zu den Ausführungen betreffend Tabelle 1, die folgende besondere Arbeitsweise:
30

35 Die ersten beiden Arbeitsphasen A.) und B.) sind die

gleichen wie in Tabelle 1, doch ergeben sich bereits folgende Abweichungen im weiteren Vorprogramm:

5 Cn.) Generieren:

Jetzt werden eine ganze Schar von Zufallszahlen z_1 bis z_n im schlüsselseitigen Zufallszahlengenerator 14 sowie eine weitere, unabhängige Schar von Zufallszahlen z'_1 bis z'_n im schloßseitigen Zufallsgenerator 24 erzeugt.

10

Dn.) Fragen und Rückfragen:

Unter Verwendung der Kommunikationsglieder 17, 27 teilen sich Schlüssel 10 und Schloß 20 gegenseitig die beiderseits generierten Zufallszahlen als Eingangsgrößen, was man als Frage des 15 Schlüssels 10 an das Schloß 20 und als Rückfrage des Schlosses 20 an den Schlüssel 10 auffassen kann.

En.) Speichern:

Die beiderseits vorliegenden beiden Scharen von Eingangsgrößen 20 z_1 bis z'_n werden nun schlüssel- und schloßseitig in den Speichern 13, 23 für das jetzt einsetzende Hauptprogramm gespeichert, wo mehrere Arbeitszyklen ablaufen.

25

Die bisher zwischen Schlüssel und Schloß 10, 20 übermittelten Fragen und Rückfragen lassen über die individuelle Kodierung des zusammengehörigen Schlüssel-Schloß-Paars nichts erkennen. Eine Dekodierung ist aber auch in den verschiedenen nachfolgenden Arbeitszyklen nicht möglich. In jedem Arbeitszyklus, der mit einheitlichen Indizes bezeichnet ist, fallen, bis auf die erste Arbeitsphase, die gleichen Vorgänge an, wie sie im Zusammenhang mit Tabelle I bereits beschrieben worden sind, und zwar:

35

F1.) Bilden der ersten Rechengröße:

Im Schlüssel 10 und im Schloß 20, jeweils für sich, werden

aus den zugehörigen Speichern 13, 23 vorzugsweise mehrere Zufallszahlen in beidseitig übereinstimmender Weise entnommen und diese jeweils nach dem gleichen Bildungsgesetz miteinander zu einer ersten Rechengröße x_1 verknüpft. Dieses
5 in den Festspeichern 12 bzw. 13 eingegebene Bildungsgesetz ist ein weiterer Teil des Kodes, welcher ein zusammengehöriges Schlüssel-Schloß-Paar 10, 20 gegenüber allen übrigen, nicht zusammengehörigen individualisiert. Im Falle der Tabelle II ist angenommen, daß ein zusammengehöriges Schlüssel-Schloß-
10 Paar vorliegt, weshalb beidseitig die gleiche Rechengröße x_1 anfällt.

In den nun folgenden Arbeitsgängen G1, H1 fallen, bezogen auf die Rechengröße x_1 die gleichen Vorgänge an, die
15 in den entsprechenden Arbeitsphasen der Tabelle I bereits ausführlich beschrieben worden sind. Dann ergibt sich die

J1.) erste Antwort:

Das Schloß 20 teilt über die Kommunikationsmittel 27, 17
20 dem Schlüssel 10 seine ermittelte Ausgangsgröße \bar{y}_1 mit. Diese Mitteilung kann aber schloßseitig, ohne daß man auf das nachfolgende Vergleichsergebnis warten müßte, bereits dazu ausgenutzt werden, um wie ausweislich der eingeziehenen "Schaltgliedsymbolik" zu ersehen ist, aus dem
25 Speicher schloßseitig bereits eine weitere Gruppe von Zufallszahl für den nächsten Arbeitszyklus zu entnehmen, auf den später einzugehen sein wird.

K1.) Vergleichen:

Dann kommt es, wie bereits in Tabelle II beschrieben wurde,
30 zu einem Vergleichen der beiderseitigen Endgrößen \bar{y}_1 in der Arbeitsphase K1, die zu den bereits erwähnten Alternativen in der Arbeitsphase

L1.) Auswahl-Folge:

35 führt, nämlich bei fehlender Übereinstimmung einen Stopp

des Arbeitsvorganges auf der Schlüsselseite und im Fall einer Übereinstimmung wird nun auch schlüsselseitig aus dem dortigen Speicher 13 aufgrund der in 12 vorgegebenen Programmsteuerung die gleiche Gruppe von Zufallszahlen wie vorstehend schloßseitig bei J1.) für die weitere Vergleichsarbeit entnommen.

Es schließen sich nun die für einen vollen Arbeitszyklus benötigten Arbeitsschritte an, wie sie aus Tabelle II zu erkennen und mit dementsprechenden Bezeichnungen F2 bis L2 bezeichnet worden sind. In den einzelnen Arbeitsphasen ergeben sich die im vorausgehenden Arbeitszyklus bereits beschriebenen Vorgänge, die zur Bildung einer entsprechenden Rechengröße x_2 auf beiden Seiten in der Arbeitsphase F2 führen und sich dann in den nachfolgenden Arbeitsphasen G2 und H2 zu den entsprechenden Ausgangsgrößen \bar{y}_2 entwickeln. Dieser zweite Arbeitszyklus läuft zwar analog aber spiegelbildlich zu den Vorgängen im vorbeschriebenen Arbeitszyklus ab. Während vorausgehend, beim ersten Arbeitszyklus, eine erste Antwort des Schloßteiles 20 an den Schlüssel 10 in der Arbeitsphase J1 erfolgte, gibt es jetzt eine vom Schlüssel 10 an das Schloß 20 gerichtete zweite Antwort in der Arbeitsphase J2 dieses zweiten Arbeitszyklus. Darin ist eine Reaktion auf die vorausgehend in der Vorstufe in der Arbeitsphase Dn sich ergebenden Fragen und Rückfragen zu sehen. Wird nach dem Vergleich in der Arbeitsphase K2 an der Stelle L2 die fehlende Übereinstimmung ermittelt, so kommt es zu einer Unterbrechnung des Arbeitsprogrammes. Diese fehlende Übereinstimmung ergibt sich, wenn ein falscher Schlüssel vorliegt, denn es wird keine oder eine falsche erste Rückantwort in der Arbeitsphase J2 übermittelt, auch wenn schloßseitig nach dem bisherigen Programm ordnungsgemäß vorgegangen wurde. Die Wirksamkeit der Schließeinrichtung kann dadurch

für eine gewisse Zeitdauer unterbrochen werden. Das zusammengehörige Schlüssel-Schloß-Paar ist weiterhin gegenüber allen übrigen dadurch individualisiert, daß außer dem bereits erwähnten übereinstimmenden Bildungs-
5 gesetz für die Ausgangsgrößen x_1 bzw. x_2 auch noch bestimmte Funktionsgleichungen und Verschleierungsregeln in den Arbeitsphasen G1, H1 bzw. G2 und H2 vorliegen. Im allgemeinen wird es genügen, im Verlauf der gesamten Vergleichsarbeit für jeden Arbeitszyklus die gleichen
10 Rechenoperationen zu verwenden, doch könnten zur weiteren Individualisierung dieses Schlüssel-Schloß-Paares in aufeinanderfolgenden Arbeitszyklen jeweils unterschiedliche Bildungsgesetze, Funktionsgleichungen und/oder Ver-
schleierungsregeln vorliegen, auch wenn natürlich inner-
15 halb eines Arbeitszyklus schlüssel- und schloßseitig je- weils der gleiche Algorithmus verwendet wird.

Diese Arbeitszyklen können sich in der geschilderten, spiegelbildlichen Weise abwechseln, wobei nach jedem
20 Arbeitszyklus zwischen Schlüssel und Schloß eine Antwort übermittelt wird, die zu einem Vergleich der beiden Teile herangezogen wird. Dazu verwendet man immer wieder andere Gruppen, aus den in den beidseitigen Speicher 13, 23 ent-
haltenden Scharen von Zufallszahl z_1 bis z_n und z'_1 bis
25 z'_n . In Tabelle II ist angedeutet, daß sich insgesamt m Antworten in m Arbeitszyklen ergeben. Sind die Über- einstimmungen lückenlos bis zu dieser Endphase fest- gestellt worden, endet also auch der Vergleich in der letzten Vergleichs-Phase K_m positiv, so fällt bei L_m
30 ein Schaltimpuls an, der auf die Umsteuerung der Stellmittel 33, 35 im Bereich des Schlosses 20 einwirkt. Damit ist die Vergleichsarbeit beendet. Das Schlüssel-Schloß-Paar steht für eine neue Wechselwirkung wieder zur Verfügung, die wieder mit der Vorstufe beginnt.

Die hier angefallenen m Antworten \bar{y}_1 bis \bar{y}_m lassen keinerlei Rückschlüsse zu, durch welche in den Arbeitsphasen F1, G1 und H1 usw. angewendeten Algorithmen das betreffende Schlüssel-Schloß-Paar individualisiert ist. Man weiß nicht einmal auf welche Rechengröße x_m sich die einzelne Antwort \bar{y}_n ergeben hat. Durch die Übermittlung sind zwar die Zufallszahlen z_1 bis z_n "abzuhören", doch weiß man nicht, auf welche Weise sie innerhalb der elektronischen Bauteile von Schlüssel und Schloß zu den erwähnten Rechengröße x_m vereinigt wurden und welche Gruppen aus dieser Zahlenschar dabei jeweils herangezogen werden. Es fehlt daher jeder Ansatz für eine Dekodierung der das Schlüssel-Schloß-Paar kennzeichnenden Größen. Der Schlüssel lässt sich nicht kopieren. Auch aus dem Zusammenspiel zwischen Schlüssel und Schloß sind keine Anhaltspunkte zur Dekodierung der Schließeinrichtung entnehmbar.

In Abwandlung der erfindungsgemäßen Schließeinrichtung wäre es möglich, diese bei Anlagen mit unterschiedlichen Funktionen auslösenden Schlüsseln zu verwenden, wie es beispielsweise bei Kraftfahrzeugschlössern mit einem Normalschlüssel und einem Sonderschlüssel bekannt ist. In diesem Fall wäre es möglich, im Anschluß an eine Arbeitsphase H der Tabelle I bzw. II noch eine Maskierung vorzunehmen, die im Fall des Sonderschlüssels beispielsweise alle Informationen der Endgröße durchläßt, beim Normalschlüssel aber nur bestimmte Stellen. Auf der Schloßseite stehen die gleichen Maskierungen zur Verfügung, weshalb in der schloßseitig nachfolgend ablaufenden Vergleichsphase, analog zu K.) von Tabelle I für die beiden unterschiedlichen Schlüssel zwei Vergleichsmöglichkeiten angeboten werden. Die vom Schlüssel kommende Antwort analog zu K.) von Tabelle I wird zunächst einem

ersten Vergleichsglied zugeführt, das im Übereinstimmungsfall mit dem Antwortsignal eines ordnungsgemäß zugeordneten Sonderschlüssels die entsprechenden Schaltimpulse für die Sonderaufgaben im Schloß abgibt, während im Nichtübereinstimmungsfall die Anfrage an ein weiteres Vergleichsglied geht, welches das eingegangene Antwortsignal mit jener Maskierung der schloßseitigen Endgröße vergleicht, die für den ordnungsgemäßen Normalschlüssel vorgesehen ist.
5 Lag schlüsselseitig ein solcher Normalschlüssel vor, so wird Übereinstimmung der zu vergleichenden Signale jetzt festgestellt und daher ein für die Funktionen des Normal-schlüssels vorgesehener Schaltimpuls im Schloß ausgelöst, der die dafür vorgesehenen Schaltbewegungen ausführt. Ist aber auch diesmal keine Übereinstimmung festgestellt wor-
10 den, so kommt es zu dem bereits im Zusammenhang mit Tabelle I bei der Arbeitsphase L.) beschriebenen Stopp des Ver-
gleichsverfahrens für wenigstens eine bestimmte Zeitdauer.

Auf diese Weise können auch mehr als nur zwei Schlüssel
20 durch entsprechend vielfältige Maskierung der Endgröße in einer Schließanlage verwenden, die von einem Schloß er-kannt und zur Auslösung unterschiedlicher Funktionen im Schloß ausgenutzt werden. Bei Kraftfahrzeugen beispiels-weise könnte man verschiedene Schlüssel für das Fahrzeug
25 steuernde, unterschiedliche Personen vorsehen, denen schloßseitig wenigstens teilweise unterschiedliche Funk-tionen zugeordnet sind. So kann man, in Abhängigkeit von dem benutzten, personenbezogenen Schlüssel, über den ent-sprechenden Schlüssel unterschiedliche Schaltimpulse im
30 Schloß auslösen, die den Rückspiegel, den Außenspiegel, die Sitzhöhe, die Sitzposition und/oder die Stellung der Rückenlehne selbsttätig an die individuellen Bedürfnisse dieser Person einstellen. Wird mit dem einer bestimmten Person zugeordneten Schlüssel z.B. das Zündschloß betätigt,
35 so wird gemäß den einprogrammierten Werten vom Schloßteil die Einstellung aller erforderlichen Bauteile an die

Bedürfnisse der betreffenden Person ausgeführt. Das Fahrzeug stellt sich selbst personengerecht ein. Durch unterschiedliche Maskierungen ist eine große Vielzahl unterschiedlicher Schlüssel bei gleichem Schloß für verschiedene Steuerfunktionen möglich.

Schließlich ist die erfindungsgemäße Schließeinrichtung auch bei Anlagen mit hierarchisch einander über- und untergeordneten Schlüsseln und Schlössern möglich, worauf bereits hingewiesen wurde. Im einfachsten Fall verwendet man bei allen Schlüsseln den gleichen Algorithmus, doch wird das Resultat in Abhängigkeit von der hierarchischen Stellung des Schlüssels bzw. des Schlosses maskiert. Je mehr übergeordnet ein Schlüssel ist, umso geringer ist die Maskierung. Der Generalhauptschlüssel wäre dann ganz unmaskiert. Schloßseitig bedeutet dies umgekehrt, daß umso mehr alternative Maskierungen für die Ausgangsgröße \bar{y} im Anschluß an die Arbeitsphase H.) der Tabelle I erforderlich sind, je untergeordneter das Schloß ist, weil es mit einer bestimmten Anzahl von gleich- und übergeordneten Schlüssel erfolgreich zusammenwirken muß. In der Vergleichsphase analog zu K.) von Tabelle I werden schloßseitig alle für dieses Schloß vorgesehenen alternativen Maskierungen berücksichtigt, bevor in der Schlußphase L.) entschieden wird, ob alle keine Übereinstimmung liefern und daher der Vergleichsvorgang gestoppt wird, oder ob eine der angebotenen Möglichkeiten die Übereinstimmung mit dem vom Schlüssel kommenden Antwortsignal \bar{y} liefert und daher ein Schaltimpuls zur Umsteuerung der schloßseitigen Sperrmittel erfolgen darf.

In Abweichungen vom vorgenannten Fall wäre es bei einer Schlüssel-Schloß-Hierarchie auch möglich, unterschiedlichen Schlüsseln unterschiedliche Algorithmen zugrundezulegen.

In diesem Fall beinhalten die Schlosser dann jeweils die Algorithmen aller zugelassenen Schlüssel und im Betätigungsfall wird schloßseitig überprüft, ob eine Übereinstimmung mit dem Algorithmus des Schlüssels vorliegt oder nicht,
5 worauf sich wieder die beiden Alternativen der Betätigung bzw. Nichtbetätigung der schloßseitigen Sperrmittel ergeben.

PATENTANWÄLTE

0098437

Dipl.-Phys. BUSE · Dipl.-Phys. MENTZEL · Dipl.-Ing. LUDEWIG
Unterdörnen 114 · Postfach 200210 · 5600 Wuppertal 2 · Fernruf (0202) 55 70 22/23/24 · Telex 8 591 606 wpat

57

5600 Wuppertal 2, den

P a t e n t a n s p r ü c h e :

- 1.) Elektronische Schließeinrichtung mit über elektrische Impulse miteinander in Wechselwirkung tretenden, schlüssel- und schloßartigen Teilen (Schlüsselteil 10, Schloßteil 20),

5

der Schloßteil (20) an einem abzuschließenden Element, wie einer Tür (31), angeordnet ist, Sperrmittel (33, 35) aufweist, nur von einem bestimmten zugehörigen Schlüsselteil (10) betätigbar ist und dadurch die Sperrmittel (33, 35) zwischen einer wirksamen und unwirksamen Stellung umsteuert (34),

10

wobei, auf einen Startimpuls hin, zumindest der Schloßteil (20) zahlenartige Eingangsgrößen in Form elektrischer Impulse erzeugt und diese dem anderen Teil (Schlüsselteil 10) zuleitet,

15

der Schlüsselteil (10) und der Schloßteil (20), jeweils für sich, eine eindeutige Zuordnung zwischen den schloß- und schlüsselseitig übereinstimmenden Eingangsgrößen einerseits und in Form elektrischer Impulse abgebaren Ausgangsgrößen andererseits auf-

20

weisen, diese Zuordnung nur bei zusammengehörigen Schlüssel- und Schloßteilen (10, 20) übereinstimmt und zu deren elektronischer Kodierung dient,

5 die beiden Impulsfolgen der schlüssel- und schloß- seitig anfallenden Ausgangsgrößen einem gemeinsamen, wenigstens im Schloßteil (20) angeordneten Vergleicher zugeführt und dort verglichen werden,

10 und der Vergleicher nur im Falle der Übereinstimmung der beiden Impulsfolgen einen auf die Umsteuerung (34) der Sperrmittel (33, 35) hin gerichteten Schalt- impuls abgibt,

15 dadurch gekennzeichnet,
daß der Startimpuls vom Schlüsselteil (10) ausgeht (A),

20 daß als Eingangsgrößen (x ; Z_1 bis Z_n ; Z'_1 bis Z'_n) eine oder mehrere willkürlich generierte Zufallszahlen dienen (D ; D_n),

25 daß die für zusammengehörige Schlüssel- und Schloß- teile (10, 20) charakteristische elektronische Kodierung zweistufig ausgebildet ist, nämlich

30 in einer ersten Stufe (G ; G_1 bis G_m) durch einen bestimmten Algorithmus vorgegebene Rechenoperationen im Schlüssel- und Schloß- teil (10, 20) umfaßt, deren Rechen-Resultat (y ; y_1 bis y_m) von den jeweils generierten Zufallszahlen abhängt,

in einer zweiten Stufe ($H; H_1$ bis H_m) aus dem Rechen-Resultat im Schlüssel- und Schloßteil (10, 20) - nach einer bestimmten, von den generierten Zufallszahlen unabhängigen Regel - jeweils ein Bruchstück ($\bar{y}; \bar{y}_1$ bis \bar{y}_m) entnimmt,

5

und daß nur diese schloß- und schlüsselseitig anfallenden Resultat-Bruchstücke ($\bar{y}; \bar{y}_1$ bis \bar{y}_m) als Ausgangsgrößen dem gemeinsamen Vergleicher (K; K₁ bis K_m) zuführbar (J; J₁ bis J_m) sind.

10

2.) Schließeinrichtung nach Anspruch 1, dadurch gekennzeichnet,

15

20

daß nach dem schlüsselseitigen Startimpuls (A, B) in einem Vorprogramm (A bis E_n), sowohl im schlüssel- als auch im Schloßteil (10, 20), jeweils für sich, eine eigene Menge (Z₁ bis Z_n; Z_{1'} bis Z_{n'}) unabhängiger Zufallszahlen generiert (C_n), einander mitgeteilt (D_n) und beidseitig jeweils gespeichert (E_n) werden,

25

und in einem nachfolgenden Hauptprogramm (F₁ bis L_m) jeweils eine übereinstimmende Gruppe aus diesen Zufallszahlen den Speichern (13, 23) entnommen und nach einem gleichen Bildungsgesetz zu Rechengrößen (x₁ bis x_m) verknüpft werden

30

und diese Rechengröße (x₁ bis x_m) erst den beidseitigen Rechenoperationen (G₁ bis G_m) zugrunde gelegt werden.

- 3.) Schließeinrichtung nach Anspruch 2, dadurch gekennzeichnet,
daß das Hauptprogramm zwischen dem Schlüssel- und
Schloßteil (10, 20) mehrere analoge aufeinanderfolgende Arbeitszyklen (F₁-L₁; bis F_m-L_m) umfaßt,
die jeweils aus einer schloß- und schlüsselseitig unabhängig ablaufenden, zweistufigen Ermittlungsphase (F₁, G₁, H₁ bis F_m, G_m, H_m) für die Ausgangsgrößen (\bar{y}_1 bis \bar{y}_m) und einer gemeinsam im Schlüssel- und Schloßteil (10, 20) ablaufenden Vergleichsphase (J₁, K₁ bis J_m, K_m) bestehen,
der im Falle der Übereinstimmung der verglichenen Ausgangsgrößen (\bar{y}_1 bis \bar{y}_m) am Ende eines Arbeitszyklus anfallende Schaltimpuls (L₁ bis L_{m-1}) zunächst jeweils nur die Bildung einer neuen Rechengröße (x₂ bis x_m) aus einer weiteren Gruppe der gespeicherten Zufallszahlen (Z₁ bis Z_n, Z_{1'} bis Z_{n'}) für den nächsten Arbeitszyklus auslöst
und erst im letzten Arbeitszyklus (F_m bis L_m) nach einer bestimmten Anzahl von Arbeitszyklen der sich ergebende Schaltimpuls (L_m) die schloßseitigen Sperrmittel (33, 35) umsteuert.
- 4.) Schließeinrichtung nach Anspruch 3, dadurch gekennzeichnet,
daß die Arbeitszyklen (F₁-L₁; bis F_m-L_m) abwechselnd in zueinander spiegelbildlichem Sinn

zwischen dem Schlüssel- und Schloßteil (10, 20) ablaufen, indem

5 die Vergleichsphase (K_1 bis K_m) der beidseitig anfallenden Ausgangsgrößen (\bar{y}_1 bis \bar{y}_m) in aufeinanderfolgenden Arbeitszyklen einmal schlüsselseitig (10) und einmal schloßseitig (20) abläuft

10 und dabei jeweils im anderen Teil (Schloß- bzw. Schlüsselteil 20, 10) bereits beim Übermitteln der Ausgangsgröße (\bar{y}_1 bis \bar{y}_m) die neue Rechengröße (x_2 bis x_m) für den nächsten Arbeitszyklus gebildet wird und dort, unabhängig vom Vergleichsergebnis (K_1 bis K_{m-1}) der neue Arbeitszyklus beginnt.

20 5.) Schließeinrichtung nach einem oder mehreren der Ansprüche 2 bis 4, dadurch gekennzeichnet,

25 daß in jedem Arbeitszyklus (F_1-L_1 ; bis F_m-L_m) schlüssel- und schloßseitig zwar stets der gleiche Algorithmus zugrunde liegt, dieser aber zyklenweise übereinstimmend im Schlüssel und Schloßteil (10, 20) veränderbar ist.

30 6.) Schließeinrichtung nach einem oder mehreren der Ansprüche 1 bis 5, dadurch gekennzeichnet,

daß im Falle fehlender Übereinstimmung in der Vergleichsphase (K_1 bis K_m) der Ausgangsgröße (\bar{y}_1 bis \bar{y}_m) der Schlüssel- und/oder Schloßteil (10, 20) wenigstens

für eine bestimmte Zeitdauer unwirksam wird.

- 5 7.) Schließeinrichtung nach einem oder mehreren der Ansprüche 1 bis 6, dadurch gekennzeichnet,

daß die elektrischen Impulse zwischen dem Schlüssel- und Schloßteil (10, 20) durch Strahlung, z.B. elektromagnetische Wellen (30), übertragen werden.

10

- 15 8.) Schließeinrichtung nach einem oder mehreren der Ansprüche 1 bis 6, dadurch gekennzeichnet,

daß die elektrischen Impulse zwischen dem Schlüssel- und Schloßteil (10, 20) durch Berührungskontakt übertragen werden.

- 20 9.) Schließeinrichtung nach einem oder mehreren der Ansprüche 1 bis 8, mit zueinander hierarchisch über- und untergeordneten Schlüssel- und Schloßteilen (10, 20),

d a d u r c h g e k e n n z e i c h n e t ,

25

daß allen Schlüssel- und Schloßteilen (10, 20) in der ersten Stufe (G; G₁ bis G_m) zur Ermittlung der Ausgangsgrößen (\bar{y}_1 bis \bar{y}_m) zwar der gleiche Algorithmus zugrunde liegt,

30

aber bei untergeordneten Schlüssel- und Schloßteilen (10, 20) in der zweiten Stufe (H; H₁ bis H_m) der Ermittlung kleinere Bruchstücke des Rechen-Resultats (y; y₁ bis y_m) übermittelt (J₁ bis J_m) und miteinander verglichen (K₁ bis K_m) werden als bei über-

35

geordneten Schlüssel- und Schloßteilen (10, 20).

- 10.) Schließeinrichtung nach einem oder mehreren der
5 Ansprüche 1 bis 8, mit zueinander hierarchisch über-
und untergeordneten Schlüssel- und Schloßteilen
(10, 20),
d a d u r c h g e k e n n z e i c h n e t ,
- 10 daß unterschiedliche Schlüsselteile (10) bei der
Ermittlung der Ausgangsgrößen (\bar{y}_1 bis \bar{y}_m) zwar zuein-
ander unterschiedliche Algorithmen und/oder Regeln
zur Bildung der Bruchstücke der Rechen-Resultate
(y_1 bis y_m) aufweisen,
- 15 aber die Schloßteile (20) jeweils die Algorithmen
und/oder Regeln aller zugelassenen Schlüsselteile
(10) beinhalten, welche in der Vergleichsphase
(K_1 bis K_m) auf ihre Übereinstimmung mit denjenigen
20 des Schlüsselteils (10) überprüft werden.

0098437

113

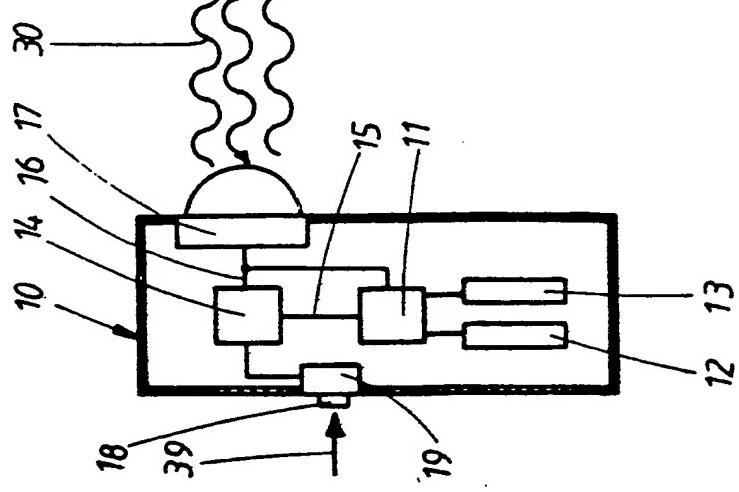
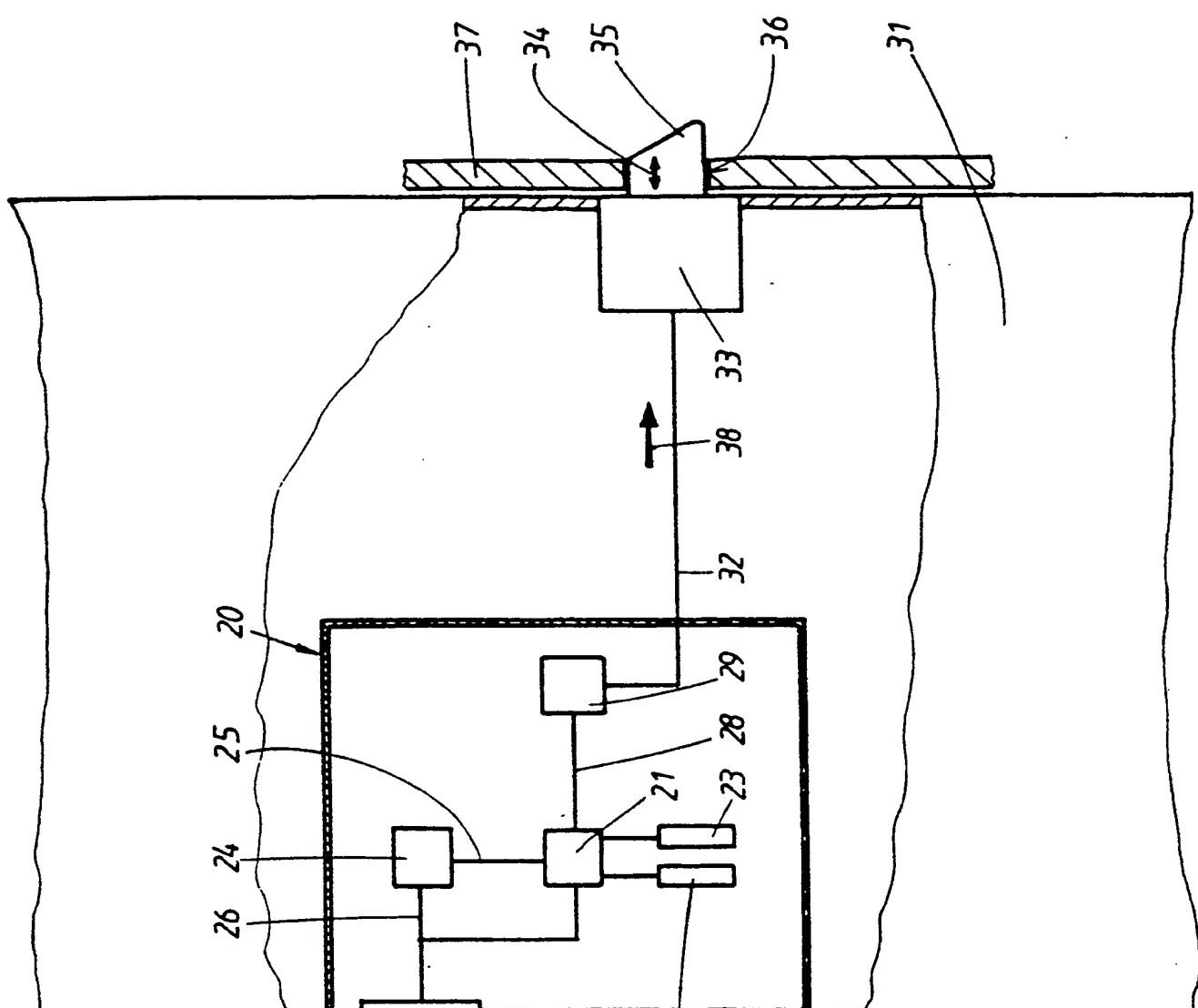


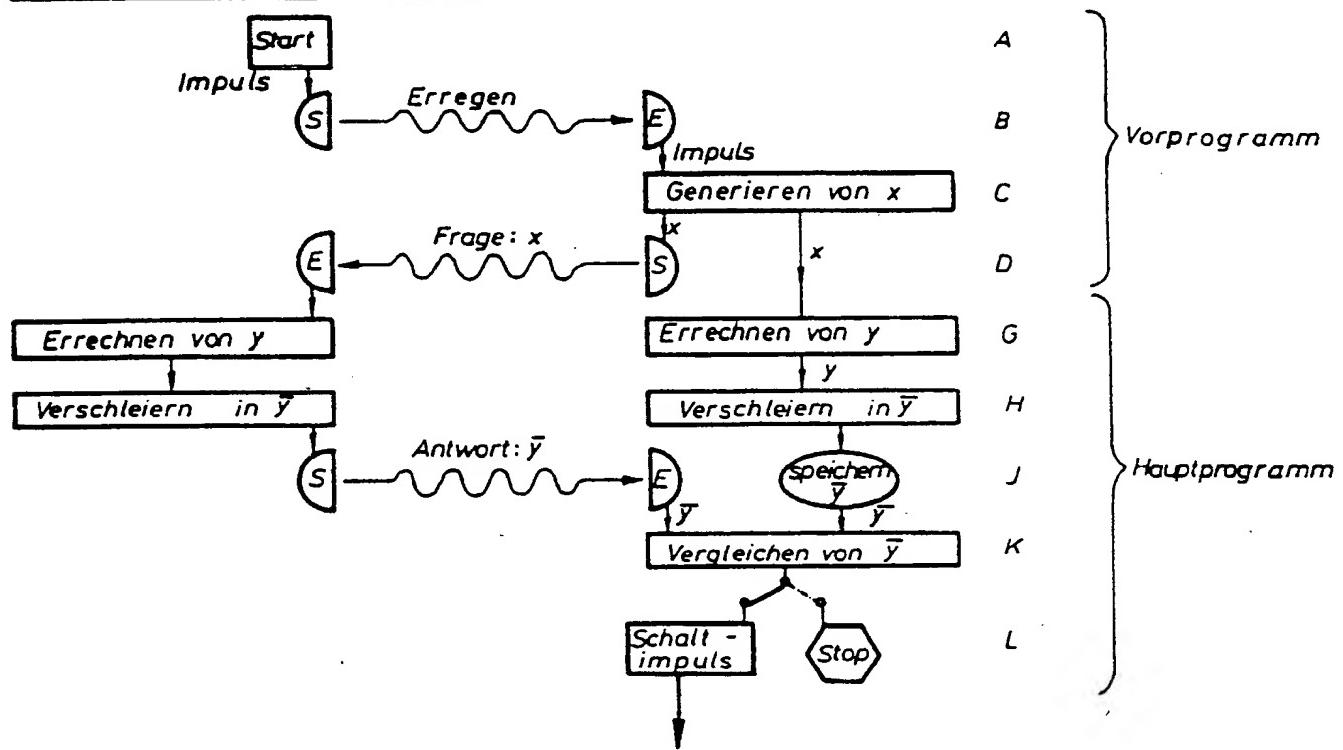
FIG. 1

2/3

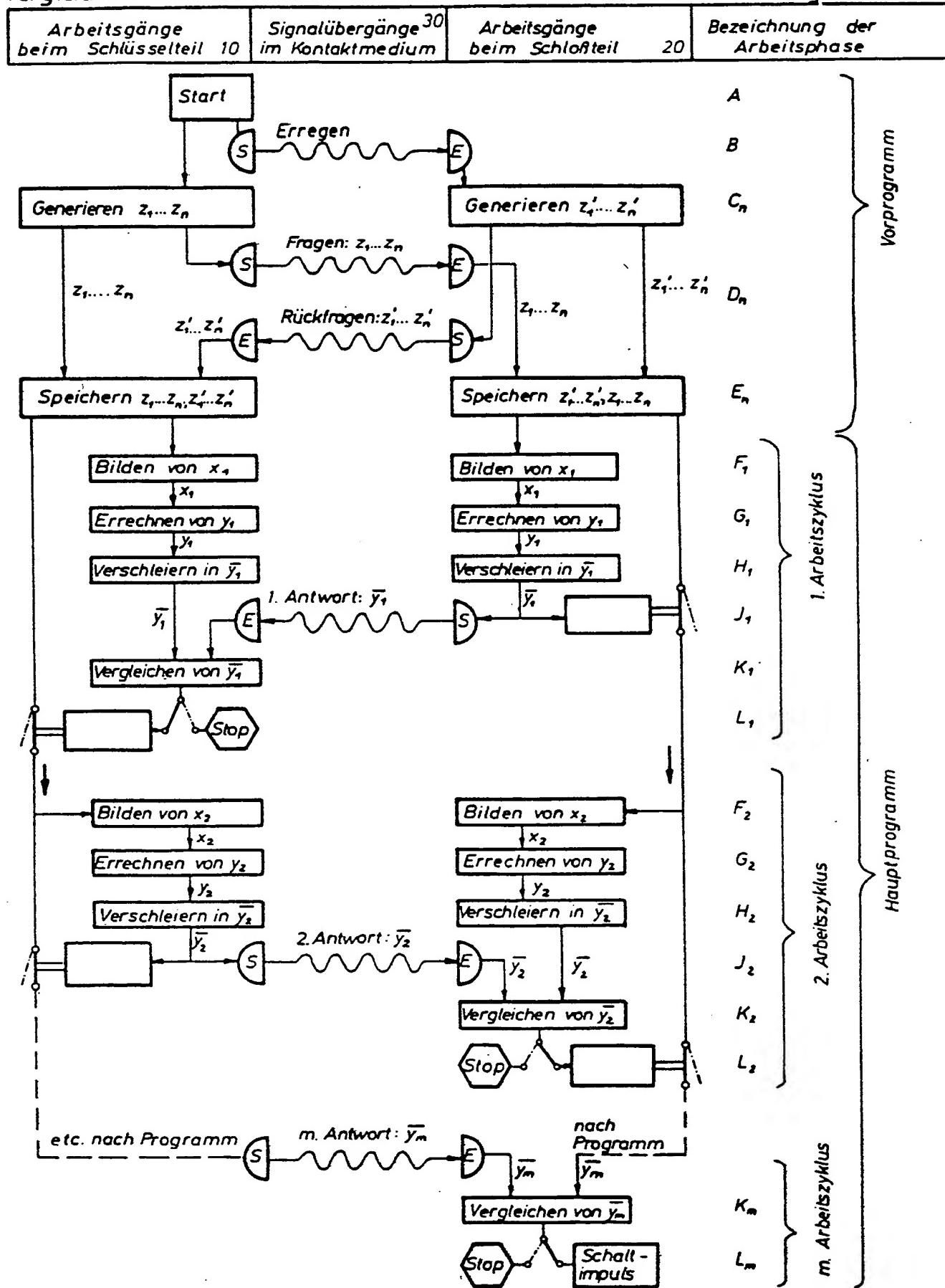
0098437

Vergleichsarbeit zwischen
Schlüssel und Schloß der Schließeinrichtung

Arbeitsgänge beim Schluesselteil 10	Signalübergänge im Kontaktmedium 30	Arbeitsgänge beim Schloßteil 20	Bezeichnung der Arbeitsphase
--	--	------------------------------------	---------------------------------



Vergleichsarbeit zwischen Schlüssel und Schloß der Schließeinrichtung



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

THIS PAGE BLANK

THIS PAGE BLANK (USPTO)